National Security Agency/Central Security Service

INFORMATION
ASSURANCE
DIRECTORATE

CGS Credential Management Capability

Version 1.1.1

A credential is means of providing evidence that supports a claim of identity, assertion, or association. Credential Management encompasses the functions to manage the creation, issuance, maintenance, revocation, reissuance, and status of each credential.

07/30/2012

CGS Credential Management Capability

Version 1.1.1

Table of Contents

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1

2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

Credentials are used as part of the authentication process, and authentication focuses on confirming a person's (or non-person's) identity, based on the reliability of his or her credential.

There are two types of individual authentication:

a) Identity authentication–Confirming a person's unique identity.
b) Attribute authentication–Confirming that the person belongs to a particular group or function (such as military veterans or U.S. citizens).

For purposes of this Capability, Credential Management refers to identity credentials only. For information on management of attributes (and application of attribute credentials), see the Attribute Management Capability.

Identity authentication can be conducted using credentials such as certificates and passwords. Certificates are digitally signed representations of an identity that are issued by a trusted authoritative source. For certificate-based credentials, the certificate is presented to support authentication. For non-certificates, such as passwords, authentication is completed by confirming that the credential applies to the user (the credential itself is the linkage between the account and the password).

3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of "good enough" when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

Credential Management begins with obtaining an identity and authenticating that identity. The identity itself is established in the Identity Management Capability, and this capability shall have an interface to be able to obtain identity information.

There shall be a degree of confidence in the credential issuance process. The confidence measure includes:

- Considerations for the identity proofing processes used during the identity registration
- Types of credential mechanisms
- Strength of the credential mechanisms and the tokens that transfer them
- Embodiment of the equipment used to access, transfer, and validate them.

For example, the lowest confidence level may begin with the user sending an e-mail request to obtain certificates. A higher confidence model may require a more stringent process such as physical presence of the requester. This confidence level is supported by the identity proofing process where credentials from other issuers are checked to establish identity, enable interoperability, and record linkages to those other identities that the user has. The confidence levels, otherwise known as assurance levels, are defined by multiple policies according to agency. The Organization shall employ the highest assurance level in identity proofing as defined by the applicable policy for that Organization (See agency-specific policies in the Directive and Policies table).

Credentials shall be issued from an internal source in the Enterprise or via an external source. To become a Certificate Authority (CA), an Organization shall document and approve all procedures in a Certificate Practice Statement (CPS). The Enterprise infrastructure needs to be designed to support the issuing of credentials. The design shall include secure communications for credential distribution and systems protections employed to protect the credential systems. No matter who issues credentials (in source or outsource), the issuer shall establish an acceptable, valid, identity management process. If the issuer employs a key-based solution (certificates), the issuer will have to have a strong key management system and rely on the Credential Management function to operate correctly to issue credentials (see Key Management for additional details).

At the time of issuance, the obtainer of the credentials shall be made aware of the proper use and handling procedures. The responsibility for protecting the credentials shall be defined and agreed upon before use.

During creation, the Credential Management function shall provide credentials that identify the holder or subject of the credential and shall bind that identity to other relevant information (e.g., issue date, expiration date), to authentication information (e.g., public key), and the issuer of the credential. The Credential Management function shall be able to use multiple identity factors in the credentials of human and non-human users to enable interoperability with external Enterprises. The multiple identity factors may include multiple types of names such as domain name or email address.

The Credential Management Capability shall support the goal of a federated and interoperable Credential Management system. At the agency level, such as Department of Defense (DoD), Intelligence Community (IC), and federal and civil levels, centralized and interoperable credentials are not always possible; however, the divisions of responsibility in Credential Management have been established (See agency-specific policies in the Directive and Policies table).

The Credential Management Capability requires a credential repository, which shall be used to provide status of the credentials (i.e., validity, expiration). Credentialing authorities shall conduct periodic audits through automation, when possible, of their credential records to sort expired or invalid credentials. The audit procedures shall be documented in a CPS which shall include provisions such as how often and what is audited. The system that maintains credential records shall have an automatic update feature, to pull records of credentials after their expiration date, or to flag them to determine if they have been renewed. Credentialing authorities for closed, controlled groups of credential holders shall also map their issued credential database periodically against a database of authorized credential holders. The Organization will provide timely and efficient credential status checking during the authentication process for all users.

Implementation of Credential Management shall include the ability to perform both a single credential revocation and a revocation of multiple credentials associated with a single identity or attribute. Both processes ensure that the request for revocation is a valid request and authenticates the requester and ensures that the requester has the authority to request a revocation. The revocation will be done quickly and efficiently, and the Organization will employ a technical mechanism to provide an efficient revocation check such as a Certification Revocation List (CRL) (see Key Management). Bulk revocation will also be supported. Bulk revocation may be necessary to revoke the credentials for everyone associated with a particular location or project.

Reissuing credentials is the final part of Credential Management. Reissue is required in the following three cases: 1) Renew, 2) Rekey, 3) Update. In each case, the Organization shall again determine the identity, authentication, and authority of the requester before renewing credentials.

4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. Within the system, credentials are public and do not contain any secret information.
2. All users have been investigated and are trusted based on their security level.
3. All persons within the Organization have been issued software/hardware identity credentials in accordance with Organizational Policy (see Directives and Policies table below).
4. Identity management provides identities to this Capability.

5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability ensures that the user is aware of and has agreed to his or her responsibilities to protect the credential.
2. The Capability issues credentials with integrity protections that can be verified.
3. The Capability provides the infrastructure to verify the validity of the credential.
4. Credentials are used to facilitate the authentication of users.
5. For non-person entities, all credentials will be software based.
6. A credential is unique to an entity, though an entity may have multiple credentials that are each unique to that entity.

6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

When the Credential Management Capability is implemented correctly, the department or agency will possess a capability to verify the identity of each of its entities (human and non-human users). For non-human users, the Organization will designate a human sponsor responsible for the device/asset. The identity of the sponsor will be authenticated via the same means as the identity of a requester, and that sponsor will be responsible for collecting the asset information, submitting the credential request, and installing the credential on the device.

The credentials used and employed by an Organization will support the goal of a federated and interoperable Credential Management system. The Organization will focus on a single ubiquitous method of Credential Management and will centralize these services to the extent possible.

A department may choose to have its credentials issued internally by the department or agency or externally. The Organization will maintain a list of credentials that are issued by that Organization. Some departments will have to defer to their overseeing agency to get credentials issued for their new users. Regardless of who issues the credentials used by an agency or Organization, an established procedure will be documented in the Organization's CPS that will be followed when credentials are either issued or revoked. The Organization will employ a mechanism for revocation of credentials and will be able to revoke a single credential or all credentials associated with a single identity. A degree of efficiency must be employed by the Organization for revocations to not inhibit operations.

Strong authentication of user access will be enabled by ensuring all user authentication is based on a minimum of possession of a hardware security token, which is sufficiently protected to allow it to be treated as an unclassified high-value item, and a secret known only by the user. No long-term secrets (i.e., Public Key Infrastructure [PKI] private keys) will be exposed outside the hardware security token. The Organization will use the highest assurance levels for identity proofing and issuing credentials.

All credentials will be generated in a secure manner including protections for the systems generating the credentials, the communications lines the credentials are passed to (if electronic), use of identity proofing, and other protections to provide assurance in the issuer and receiver. The generation process will be audited periodically to ensure its sustained security according to the CPS.

In all implementations that use credentials managed by this Capability, secure access will be available to any necessary servers to provide the most up-to-date revocation information. The Organization will ensure high availability or redundant connections for servers providing revocation information.

Credentials will be archived for business continuity purposes, such as accessing emails or files encrypted with an older key. The Organization will maintain records of revocations, renewals, and updates to credentials. The retention policy for these records will be established in the CPS.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Identity Management–The Credential Management Capability relies on the Identity Management Capability to obtain an authenticated identity to issue identity credentials.
- Key Management–The Credential Management Capability relies on the Key Management Capability to manage keys that are used as a type of credential.
- Attribute Management–The Credential Management Capability relies on the Attribute Management Capability to manage attributes that are used as a type of credential.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management–The Credential Management Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards–The Credential Management Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.
- IA Awareness–The Credential Management Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.

- IA Training–The Credential Management Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Credential Management Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Data Protection–The Credential Management Capability relies on the Data Protection Capability to provide protection mechanisms for credentials.
- Risk Mitigation–The Credential Management Capability implements individual countermeasures that may be selected by the Risk Mitigation Capability.

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	**Related Text**
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*	
IA-4 *IDENTIFIER MANAGEMENT*	Enhancement/s: (2) The organization requires that registration to receive a user ID and password include authorization by a supervisor, and be done in person before a designated registration authority. (3) The organization requires multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics be presented to the registration authority.
IA-5 *AUTHENTICATOR MANAGEMENT*	Control: The organization manages information system authenticators for users and devices by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;

	b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators upon information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); g. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type]; h. Protecting authenticator content from unauthorized disclosure and modification; and i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators. Enhancement/s: (1) The information system, for password-based authentication: (a) Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type]; (b) Enforces at least a [Assignment: organization-defined number of changed characters] when new passwords are created; (c) Encrypts passwords in storage and in transmission; (d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; and (e) Prohibits password reuse for [Assignment: organization-defined number] generations. (2) The information system, for PKI-based authentication: (a) Validates certificates by constructing a certification path with status information to an accepted trust anchor; (b) Enforces authorized access to the corresponding private key; and

	(c) Maps the authenticated identity to the user account. (3) The organization requires that the registration process to receive [Assignment: organization-defined types of and/or specific authenticators] be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor). (4) The organization employs automated tools to determine if authenticators are sufficiently strong to resist attacks intended to discover or otherwise compromise the authenticators. (5) The organization requires vendors and/or manufacturers of information system components to provide unique authenticators or change default authenticators prior to delivery. (6) The organization protects authenticators commensurate with the classification or sensitivity of the information accessed. (7) The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.
IA-7 *CRYPTOGRAPHIC MODULE AUTHENTICATION*	Control: The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. Enhancement/s: None Specified

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Credential Management Directives and Policies

Title, Date, Status	**Excerpt / Summary**
Intelligence Community (IC)	
Intelligence Community Public Key Infrastructure (PKI) Overarching Policy for the SCI Fabric, 25	Summary: It is the policy of the Intelligence Community (IC) that a single-root, hierarchical Public Key Infrastructure (PKI) be established for use on Sensitive Compartmented Information (SCI) networks between members of the

October 1999, Classified	Community. The IC PKI will provide IC member organizations, for those applications that require them, strong identification and authentication, data integrity, digital signature, non-repudiation, and encryption services for all information system-based communications and services traversing Community SCI networks. These services shall be used for communications and services between IC member organizations and those organizations and their customers.
Intelligence Community Certificate Policy, Version 4.3.3, 25 September 2008, Classified	Summary: This document provides uniform policy guidance and requirements for ensuring interoperability between Certification Authorities (CAs) within the IC PKI. It establishes standard operating policies and procedures to be used by IC agencies/components for services between members of the U.S. IC, IC customers, and others as approved by the Information and Technology Governance Board (ITGB) and the Intelligence Community Chief Information Officer (IC CIO). IC PKI public certificates and associated private keys have applicability to areas such as, but not limited to, confidentiality of information, digital signatures, and identification and authentication of individuals, as well as information system infrastructure components.
Intelligence Community Policy Guidance (ICPG) 500.1, Digital Identity 7 May 2010, Classified	See CGS Classified Annex.
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoDD 1000.25, DoD	Summary: The Personnel Identity Protection (PIP) shall be

Personnel Identity Protection (PIP) Program, 23 April 2007, Unclassified	the Department of Defense's (DoD) program for … establishing a secure and authoritative process for the issuance and use of identity credentials in the Department of Defense … and ensuring that … access to DoD physical and logical assets is granted based on authenticated and secure identity information. It establishes policy for the implementation and operation of the PIP program to include use of authoritative identity information, issuance and use of DoD identity credentials, …
DoDI 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 1 April 2004, Unclassified	Summary: This instruction implements policy, assigns responsibilities, and prescribes procedures for developing and implementing a department-wide PKI and enhancing the security of DoD information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption. It aligns DoD PKI and PK-enabling activities with DoD Directive 8500.1, as implemented by DoD Instruction 8500.2, and the DoD Common Access Card (CAC) program, as specified by DoD Directive 8190.3.
U.S. DoD X.509 Certificate Policy, Version 10.1, 19 February 2010, Unclassified	Summary: This document defines the creation and management of Version 3 X.509 public-key certificates for use in applications requiring communication between networked computer-based systems. Such applications include, but are not limited to, electronic mail; transmission of unclassified and classified information; signature of electronic forms; contract formation signatures; and authentication of infrastructure components such as web servers, firewalls, and directories. The network backbone for these network security products may be unprotected networks such as the Internet or Nonclassified Internet Protocol Router Network (NIPRNET), or protected networks such as the Secret Internet Protocol Router Network (SIPRNET).
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	

Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 1.0, 10 November 2009, Unclassified	Summary: This document outlines a common framework for Identity, Credential, and Access Management (ICAM) within the Federal Government and provides supporting implementation guidance for program managers, leadership, and stakeholders planning to execute a segment architecture for ICAM management programs. It includes courses of action, planning considerations, and technical solution information across multiple federal programs spanning the disciplines of ICAM. Federal Identity, Credential, and Access Management (FICAM) by its very nature addresses credentials and describes the business need and fit of credentialing more than the technical specifics.
X.509 Certificate Policy for the Federal Bridge CA, Version 2.15, Unclassified	Summary: This Certificate Policy (CP) defines seven certificate policies for use by the Federal Bridge Certification Authority (FBCA) to facilitate interoperability between the FBCA and other entity PKI domains. The policies represent five different assurance levels (Rudimentary, Basic, Medium, Medium Hardware, and High) for public key certificates. The level of assurance refers to the strength of the binding between the public key and the individual whose subject name is cited in the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.
X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, V1.10, Unclassified	Summary: This is the policy framework governing the PKI component of the Federal Enterprise Architecture. The policy framework incorporates six specific certificate policies: a policy for users with software cryptographic modules, a policy for users with hardware cryptographic modules, a policy for devices, a high-assurance user policy, a user authentication policy, and a card authentication policy.
Executive Branch (EO, PD, NSD, HSPD, …)	
Homeland Security Presidential Directive/HSPD-12, Policy for a Common	Summary: The directive establishes a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor

Identification Standard for Federal Employees and Contractors, 27 August 2004	employees).
Legislative	
Nothing found	

Credential Management Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Intelligence Community Public Key Infrastructure (PKI) Interface Specification (Draft), Version 2.9.4, September 2009, Classified	Summary: This specification describes the interfaces to the IC PKI, defines the interface requirements for creating X.509 Version 3 (V3) certificates and X.509 Version 2 (V2) Certificate Revocation Lists (CRLs), provides a baseline for IC PKI certificate profiles (largely mirroring those of the DoD's PKI certificate profiles), and establishes the content for PKI certificates.
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
DoD, Public Key Infrastructure Functional Interface Specification, Version 2.0, June 2007, Unclassified	Summary: This specification describes the functional interface to the DoD PKI. The purpose of the specification is to provide information to allow various organizations to acquire or develop applications that will be capable of interacting with and using the DoD PKI.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
NIST SP 800-32, Introduction to Public Key Technology and the	Summary: This special publication was developed to assist agency decision-makers in determining whether a PKI is appropriate for their agency, and how PKI services can be

Federal PKI Infrastructure, Unclassified	deployed most effectively within a federal agency. It is intended to provide an overview of PKI functions and their applications. Additional documentation will be required to fully analyze the costs and benefits of PKI systems for agency use, and to develop plans for their implementation. This document provides a starting point and references to more comprehensive publications.
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, …)	
Nothing found	

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Scope of work–The number of users and devices that need credentials will affect the overall complexity of managing credentials.

2. Solution used for implementation–Internally versus externally managed solutions will change the cost structure. The Enterprise may need to supply hardware tokens.
3. Cost of operating the registration system–The Enterprise needs to provide CAs, Registration Authorities (RAs), registration authority workstations, and end-user workstation readers.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Credential Management Capability.

- The Enterprise shall manage the creation, issuance, maintenance, revocation, reissuance, and status of credentials. Credentials are used as part of the authentication process, which focuses on confirming a person's (or non-person's) identity, based on the reliability of their credential.
- The Enterprise credential management system shall interface with identity management and access management systems to authenticate personnel prior to issuing credentials to them.
- The Enterprise shall have a degree of confidence in the credential issuance process, which includes confidence measures such as consideration for the identity proofing process, types of credential mechanisms, strength of the credential mechanism, and equipment used to validate the credential.
- All credentials shall be issued from an authorized source that may be internal or external to the Organization.
- To become a CA, an Organization shall document and approve all procedures in a CPS.
- The Enterprise infrastructure shall support secure mechanisms for distributing credentials.
- System protection mechanisms shall be employed to protect credential management systems.
- Credential issuers shall establish an acceptable, valid identity management process.
- When key-based credential solutions are used, the issuer shall use a strong key management system.

- Personnel who have been issued credentials shall receive appropriate training on the proper credential use and protection procedures.
- The credential management system shall provide credentials that identify the holder or subject of the credential and shall bind that identity to other relevant information (e.g., issue date, expiration date), to authentication information (e.g., public key), and the issuer of the credential when credentials are created.
- The credential management system shall be able to use multiple identity factors in the credentials of human and non-human users to enable interoperability with external Enterprises.
- The Enterprise shall manage credentials such that they support the goal of a federated and interoperable system that works across Enterprise boundaries as established by Community policy.
- The Enterprise shall operate a credential repository, which shall provide the status of credentials (i.e., validity, expiration).
- Credential management system audit procedures shall be documented in a CPS.
- Credential management system periodic audits of its credential records to sort expired or invalid credentials shall be automated, when possible.
- Credential management systems shall have a feature by which to automatically update its records for reasons such as credential expiration or renewal.
- Credentialing authorities for closed or controlled groups shall map their credential database against a database of authorized credential holders.
- Credential status checks performed during user authentication shall be provided in a timely and efficient manner.
- The credential management system shall be able to perform single and multiple (i.e., bulk) credential revocation.
- The credential management system shall authenticate the originator of all revocation requests.
- The Enterprise shall provide an efficient technical mechanism by which to perform credential revocation checks such as a CRL.
- The credential management system shall reissue credentials, as necessary, in the following three cases: 1) renew, 2) rekey, 3) update.
- The credential management system shall determine the identity, authentication, and authority of the requester before renewing credentials.